IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF: ALL CONTENT AND OTHER INFORMATION ASSOCIATED WITH DISCORD ACCOUNT "TOASTY" WITH USER ID: 485907045237653505 MAINTAINED AT PREMISES CONTROLLED BY DISCORD INC.	Case No. 1:23-mj-00019-WCM **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Theresa Wellens, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am investigating the activities of the social media account belonging to Landon Carter PUTT (SUBJECT), who resides at 105 11th Street NE, Hildebran, North Carolina, 28637 (SUBJECT RESIDENCE) and uses the Discord ID: 485907045237653505 and Discord username: Toasty (SUBJECT ACCOUNT) and email accounts landoncputt@gmail.com (EMAIL ACCOUNT 1) and landonspark07@gmail.com (EMAIL ACCCOUNT 2). As will be shown below, there is probable cause to believe that SUBJECT used his Discord social media account to possess and distribute child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (a)(5)(B). I submit this Application and Affidavit in support of a search warrant authorizing a search of SUBJECT ACCOUNT pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), as there is probable cause to believe that SUBJECT ACCOUNT, maintained at premises controlled by Discord, contain evidence, fruits, and instrumentalities of the forgoing criminal violations, all as specified in Attachment B hereto, which relate to the knowing transportation, receipt, possession, and distribution of child pornography.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since 2017. I am presently assigned to the Hickory Resident Agency (RA) within the Charlotte Division. While employed by the FBI, I have investigated federal criminal violations related to child exploitation, and child pornography. I have gained experience through training and everyday work relating to conducting these types of investigations. I have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 2252A, and I am authorized by the Attorney General to request a search warrant.

3. I am a federal law enforcement officer within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant and make arrests. Additionally, I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7) and am empowered by 18 U.S.C § 3052 to conduct investigations of, and to make arrests for, violations of federal criminal statutes.

4. The facts set forth in this Affidavit come from my personal observations, my training and experience, evidence gathered pursuant to subpoenas, government records requests, and information obtained from other agents and witnesses. Because this Affidavit is submitted for the limited purpose of establishing probable cause to support the contemporaneously filed Applications, it does not include each and every fact known to me or to other investigators.

5. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of the violation of

Title 18 U.S.C. § 2252A, transportation, access with intent to view, possession, receipt, and distribution of child pornography are presently located within SUBJECT ACCOUNT.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of Title 18, U.S.C. § 2252A(a)(2)(A) and (a)(5)(B), relating to material involving the sexual exploitation of minors.

a. Title 18 U.S.C. § 2252A(a)(2)(A) makes it a crime to knowingly receive or distribute (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

b. Title 18, U.S.C. § 2252A(a)(5)(B) prohibits knowingly possessing or knowingly accessing with intent to view any book, magazine, periodical, film, video tape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of

themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

c. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards,

printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It

commonly includes programs to run operating systems, applications, and utilities.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. Like a phone number, no two computers or network of computers connected to the internet are assigned the same IP address at exactly the same date and time. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

i. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

j. "Sexually explicit conduct" refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

k. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

l. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

9. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

10. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

13. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example,

by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

BACKGROUND INFORMATION ON DISCORD

15. In my training and experience, I have learned that Discord provides on-line service for communication including messaging, voice calls, and video calls, which is available to the public. Discord allows subscribers to obtain and utilize their services by downloading an application to their mobile devices. Subscribers obtain an account by downloading the application and registering with Discord. During the registration process, Discord asks subscribers to provide basic personal information. Therefore, the computers of Discord are likely to contain stored electronic communications and information concerning subscribers and their use of Discord services, such as account access information, messaging transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

16. Affiant has researched whether Discord retains digital evidence and has learned that Discord does retain all digital evidence unless the parties using the application themselves delete the information. In general, a message that is sent between Discord subscribers is stored in the subscriber's received messages box until the subscriber deletes the message. If the subscriber does not delete the message, the message can remain on servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Discord's servers for a certain period of time. Affiant also learned that Discord can provide device identifying features, a record of all devices a user uses to access Discord, all images and videos the account has distributed and received, contact lists by user name and user identification, VOIP data and IP addresses the account has used to access Discord, approximate geo-location of account devices, any applicable social media integration data, and user activity logs.

17. In my training and experience, messaging application providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

18. In my training and experience, messaging application services typically retain certain transactional information about the creation and use of each account on their systems.

This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the messaging account.

19. In my training and experience, in some cases, messaging service users will communicate directly with the messaging service provider about issues relating to the account, such as technical problems, or complaints from other users. Messaging service providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. As explained herein, information stored in connection with messaging service account may provide crucial evidence of the "who, what, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with messaging account can indicate who has used or

controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, messaging communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the messaging service provider can show how and when the account was accessed or used. For example, as described below, messaging service providers typically log the Internet Protocol (IP) addresses from which users access the messaging account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the messaging account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the messaging account owner's state of mind as it relates to the offense under investigation. For example, information in a messaging account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

FACTS IN SUPPORT OF PROBABLE CAUSE

21. On or about December 28, 2022, the FBI Hickory Field Office working in partnership with a foreign government, was notified that from on or about September 2021, through to one or about March 2022, a minor victim (V1) in the foreign country was

communicating with SUBJECT who was requesting V1 to create and send child pornography material. Additionally, SUBJECT was enticing V1 to harm themselves. In their communications, SUBJECT expressed knowledge that of V1 was 14 years old and that what the SUBJECT was asking V1 to do was a crime in both the SUBJECT's and V1's respective countries. Law enforcement with the foreign government identified the SUBJECT as using the Discord username Toasty (SUBJECT ACCOUNT) and email accounts landoncputt@gmail.com (EMAIL ACCOUNT 1) and landonspark07@gmail.com (EMAIL ACCCOUNT 2). Law enforcement with the foreign government voluntarily received Discord chats between V1 and the SUBJECT ACCOUNT. From the chats, the foreign government law enforcement identified that V1 had sent child sexual abuse images to SUBJECT ACCOUNT. Additionally, SUBJECT ACCOUNT stated to V1 during a chat that SUBJECT ACCOUNT had saved every "nude" that V1 had sent to the SUBJECT ACCOUNT.

22. On or about January 27, 2023, your Affiant served Discord Inc. with an administrative subpoena requesting subscriber information regarding the SUBJECT ACCOUNT.

23. On or about January 30, 2023, the FBI Hickory Field Office received the following information from Discord, Inc. regarding, SUBJECT ACCOUNT:

User ID: 485907045237653505

Username: Toasty #9307

Email: landoncputt@gmail.com(verified)

Phone number: +1-828-390-8422

Registration (UTC): September 2, 2018 20:21:07

Most recent IP Address: 172.220.140.204 (DISCORD IP ADDRESS) on January 24, 2023 15:39:26 UTC

Billing Name: Landon Putt

Billing Address: 105 11th Street NE, Hildebran, North Carolina 28637

24. On or about February 10, 2023, your Affiant served Charter Communications with an administrative subpoena requesting subscriber information regarding IP address 172.220.140.204, for January 24, 2023, at 12:00AM EST.

25. On or about February 15, 2023, the FBI Hickory Field Office received the following information from Charter Communications, through an administrative subpoena regarding IP address 172.220.140.204:

Target details: 172.220.140.204, 1/24/2023 12:00AM Eastern

Subscriber Name: Jessica Putt

Service Address: 105 11th Street NE, Hildebran, NC 28637

User Name or Features: JESSICALPUTT@GMAIL.COM,

JPUTT01@SPECTRUM.NET

Account Phone Number: 828-640-0972

Account Number: 8351400280799966

MAC: 5CFA25BCC967

Lease Log: Start Date: 11/29/2022 05:01 AM ; End Date: 02/06/2023 07:13PM

26. Accurint, a database available to law enforcement, contained information confirming that SUBJECT resided at 105 11th Street NE, Hildebran, NC 28637 since June 2013 through January 2023.

27. On February 2, 2023, a Department of Motor Vehicle Records Search revealed a valid North Carolina driver's license, NC DL: 45219581, issued to Landon Carter PUTT

(SUBJECT), residence 105 11th Street NE, Hildebran, NC 28637, with a date of birth of April 19, 2002. The SUBJECT's date of birth reveals he was an adult during the time he engaged in the receipt of child pornography.

CONCLUSION

28. Based on the aforementioned information, your Affiant respectfully submits that there is probable cause to believe that SUBJECT acted through SUBJECT's ACCOUNT to receive, possess, and distribute child pornography. Your Affiant respectfully submits that there is probable cause to believe that SUBJECT has violated 18 U.S.C. §§ 2252A. Additionally, there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 2252A(a)(2)(A) and (a)(5)(B), is located within SUBJECT ACCOUNT described in Attachment A, and this evidence, listed in Attachment B to this Affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

This affidavit was reviewed by AUSA Alexis Solheim.

/S/ Theresa Wellens
Date: March 9, 2023
Special Agent
Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 9th day of March, 2023, at 11:54 AM

Signed: March 9, 2023

W. Carleton Metcalf
United States Magistrate Judge

ATTACHMENT A

Subject Account and Execution of Warrant

This warrant is directed to Discord, Inc. (the "Provider" or "Discord"), headquartered at 444 De Haro Street, Suite 200, in San Francisco, California, and applies to all content and other information within the Provider's possession, custody, or control associated with the following Discord Account:

User ID	**485907045237653505**
Username	**Toasty #9307**
Email	**landoncputt@gmail.com**

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Attachment B below.

ATTACHMENT B

Information to be Produced by the Provider

I. Information to be disclosed by Discord, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any messages, images, videos, emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the **SUBJECT ACCOUNT** listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, Discord passwords, Discord security questions and answers, alternate Discord accounts, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

b. The contents of all messages associated with the account, including stored or preserved copies of messages sent to and from the account, draft messages, the source and destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message;

c. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have been sent to this user ID;

d. The types of service utilized to include alternative Discord, Inc. communication methods or platforms;

e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

g. All past and present communication lists of other Discord, Inc. users communicating with this account;

h. The types of service utilized by the user;

i. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

j. All records pertaining to communications between this Discord account and any person regarding the user or the user's Discord account, including contacts with support services and records of actions taken.

k. Discord, Inc. shall disclose responsive data, if any, by sending to FBI SA Theresa Wellens, 231 Government Ave SW, Suite 303, Hickory, North Carolina 28603, using the US Postal Service or another courier service, notwithstanding 18 U.S.C. § 2252A or similar statute or code.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, § 2252A(a)(2)(A) and (a)(5)(B) for the time period **September 1, 2021,** to the date of the execution of the search warrant, for the **SUBJECT ACCOUNT** listed in Attachment A pertaining to the following matters, including attempting to engage in the following matters:

(a) The production, distribution and possession of child pornography, and evidence indicating attempts to commit these offenses or planning to commit these offenses, to include communications with victims and potential victims, and communications with and among distributors, potential distributors, recipients or potential recipients of child pornography.

(b) All records or information in the **SUBJECT ACCOUNT** and maintained regarding the creation and use of the Accounts, including Basic Subscriber Information, Discord username, E-mail address, phone number, Discord Account Creation information, Timestamp and IP address logins and logouts, address books, contact lists, telephone numbers.

(c) Evidence of utilization of other email accounts, social media accounts, online chat programs, file storage accounts, including any account or usernames.

(d) Messages, communications, records, and files associated with or attached to email messages, and transactional data that constitutes evidence of, that may have been used to facilitate, and that were capable of being used to commit or further

violations of the above-reference code sections, and to create, access, or store evidence of such crimes.

(e) Information relating to who created, used, and communicated with the **SUBJECT ACCOUNT**, including records about their identities and whereabouts.

(f) Information indicating how and when the **SUBJECT ACCOUNT** was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account user(s).

(g) Information indicating the geolocation of the **SUBJECT ACCOUNT** and any information identifying the location of the user.

(h) Evidence indicating the **SUBJECT ACCOUNT** owner's and user's state of mind as it relates to the crimes under investigation.

(i) All records, documents, invoices, or materials associated with the **SUBJECT ACCOUNT** that concern accounts with an Internet service provider or a telephone service provider whose services may have been used in the commission of the above-reference code sections and crimes.

(j) Evidence of utilization of aliases and fictitious names.